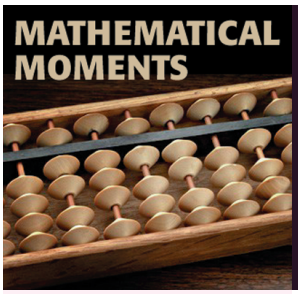

Unlocking the Secrets of AI

metamorworks / iStock / Getty Images Plus via Getty Images

"AI used to bring up visions of robots walking around impersonating humans," said Kristin Lauter, director of FAIR Labs North America (formerly Facebook AI Research). But in recent years, artificial intelligence has become more familiar, and less fantastical. It's given us movie recommendations, chatted with us on ChatGPT, and beaten us at online chess. It's also diagnosed conditions such as skin cancer or heart disease. "Today we have a more focused vision of what AI is, and it's not necessarily embodied," added Lauter. "It can just be a computer taking actions on behalf of humans, based on data about the world that it has been trained on."

In 2022, Lauter and two interns joined a growing group of researchers applying AI to cryptography. Online, private information is secured using difficult-to-solve math problems. Researchers must test those problems thoroughly to be sure they are truly difficult — if hackers can solve the problem, they'll have access to your information. Lauter and her coauthors introduced a machine learning strategy for attacking one well-known cryptography problem called "learning with errors." Their strategy, called SALSA (**S**ecret-recovery **A**ttacks on **L**earning with Errors via **S**equence-to-sequence models with **A**ttention), can't yet unlock our credit card numbers. But one of the iterations was successful enough that Lauter's team notified the National Institute of Standards and Technology, the organization responsible for standardizing the "learning with errors" cryptography scheme.

References:

"SALSA FRESCA: Angular Embeddings and Pre-Training for ML Attacks on Learning With Errors." Samuel Stevens et al, *Cryptology ePrint Archive*, 2024; 150.

"SALSA VERDE: a machine learning attack on learning with errors with sparse small secrets." Cathy Yuanchen Li et al, NIPS '23: *Proceedings of the 37th International Conference on Neural Information Processing Systems*. 2024; 2322: 53343–53361.

"Heterogeneous Training Cluster with Ray at Netflix." Pablo Delgado and Lingyi Liu. 2023. Abstract accessed 2024.

"Machine learning: applications of artificial intelligence to imaging and diagnosis." James A. Nichols, Hsien W. Herbert Chan, and Matthew A. B. Baker. *Biophys.* Rev. 2019; 11(1): 111—118.

"Evaluation of artificial intelligence techniques in disease diagnosis and prediction." Nafiseh Ghaffar Nia, Erkan Kaplanoglu, and Ahad Nasab. *Discov. Artif. Intell.* 2023; 3(1): 5.

Watch an interview with an expert!

MM/172

AMS American Mathematical Society

*The **Mathematical Moments** program promotes appreciation and understanding of the role mathematics plays in science, nature, technology, and human culture.*

www.ams.org/mathmoments